

# EUROPEAN PATENT OFFICE

## Patent Abstracts of Japan

PUBLICATION NUMBER : 2000113587  
PUBLICATION DATE : 21-04-00

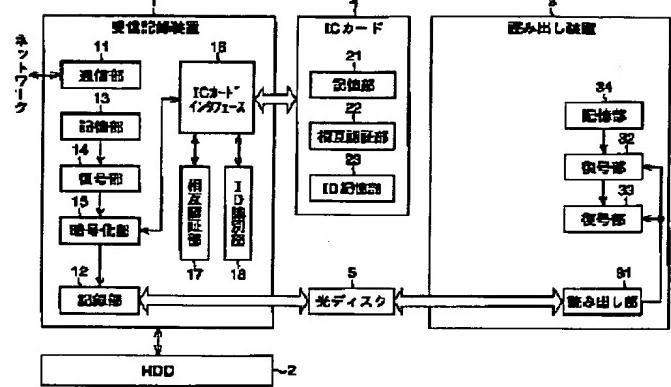
APPLICATION DATE : 05-10-98  
APPLICATION NUMBER : 10282226

APPLICANT : SONY CORP;

INVENTOR : KITAHARA ATSUSHI;

INT.CL. : G11B 20/10 G09C 1/00 H04L 9/14  
H04L 9/32

TITLE : RECORDING DEVICE AND ITS  
METHOD, DECRYPTION DEVICE AND  
ITS METHOD, PROVISION MEDIUM AS  
WELL AS INFORMATION RECORDING  
MEDIUM



ABSTRACT : PROBLEM TO BE SOLVED: To enable the utilization of encrypted information in devices exclusive of a device to which the information is supplied while preventing the illicit utilization thereof by executing mutual authentication with an information memory medium, encrypting a first key with a second key and recording the encrypted information and the encrypted first key to the memory medium.

SOLUTION: An encryption section 15 reads a key for movement out of the memory section 21 of an IC card 4, again encrypts the decrypted content key with the key for movement and records the key on an optical disk 5. When the ID read out of the ID memory section 23 of the IC card 4 is decided to be not registered in an ID identification section 18 and is decided to be not mutually authenticated with the IC card 4, the ID identification section 18 or a mutual authentication section 17 executes prescribed error processing. The mutual authentication section 17 decrypts received random numbers with the previously stored common key and if the random numbers coincide with the random numbers before the encryption, the IC card 4 is authenthicated as the correct IC card.

COPYRIGHT: (C)2000,JPO

|                           |       |               |                   |
|---------------------------|-------|---------------|-------------------|
| (51) Int.Cl. <sup>7</sup> | 識別記号  | F I           | テマコード*(参考)        |
| G 1 1 B 20/10             |       | G 1 1 B 20/10 | H 5 D 0 4 4       |
| G 0 9 C 1/00              | 6 6 0 | G 0 9 C 1/00  | 6 6 0 D 5 K 0 1 3 |
| H 0 4 L 9/14              |       | H 0 4 L 9/00  | 6 4 1             |
| 9/32                      |       |               | 6 7 5 A           |

審査請求 未請求 請求項の数12 O L (全 11 頁)

|          |                        |         |   |
|----------|------------------------|---------|---|
| (21)出願番号 | 特願平10-282226           | (71)出願人 | 000002185<br>ソニー株式会社<br>東京都品川区北品川6丁目7番35号 |
| (22)出願日  | 平成10年10月5日 (1998.10.5) | (72)発明者 | 石橋 義人<br>東京都品川区北品川6丁目7番35号 ソニ<br>ー株式会社内   |
|          |                        | (72)発明者 | 浅野 智之<br>東京都品川区北品川6丁目7番35号 ソニ<br>ー株式会社内   |
|          |                        | (74)代理人 | 100082131<br>弁理士 稲本 義雄                    |
|          |                        |         |   |

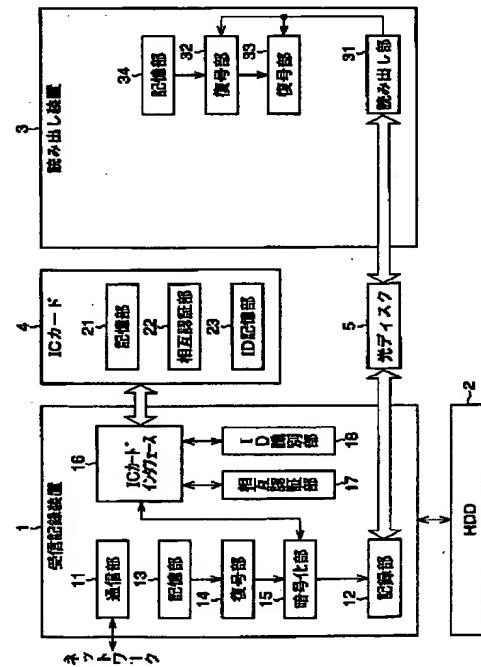
最終頁に続く

(54)【発明の名称】 記録装置および方法、復号装置および方法、提供媒体、並びに情報記録媒体

## (57)【要約】

【課題】 不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用できる。

【解決手段】 相互認証部17は、ICカード4と相互認証する。暗号化部15は、移動用鍵で、コンテンツ鍵を暗号化する。記録部12は、暗号化されたコンテンツ、および暗号化部15により暗号化されたコンテンツ鍵を光ディスク5に記録する。



**【特許請求の範囲】**

**【請求項 1】** 暗号化された情報、および前記情報を復号する第1の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第2の鍵を記憶する情報記憶媒体が装着される、記録装置において、  
前記情報記憶媒体と相互認証する相互認証手段と、  
前記相互認証手段による前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第2の鍵で、前記第1の鍵を暗号化する暗号化手段と、  
前記暗号化された情報、および前記暗号化手段により暗号化された前記第1の鍵を前記記録媒体に記録する記録手段とを備えることを特徴とする記録装置。

**【請求項 2】** 前記情報記憶媒体は、前記記録媒体に記録された情報を読み出しする読み出し装置を特定するデータをさらに記憶し、  
前記読み出し装置を特定するデータを識別する識別手段をさらに備えることを特徴とする請求項1に記載の記録装置。

**【請求項 3】** 暗号化された情報、および前記情報を復号する第1の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第2の鍵を記憶する情報記憶媒体が装着される、記録装置の記録方法において、  
前記情報記憶媒体と相互認証する相互認証ステップと、  
前記相互認証ステップでの前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第2の鍵で、前記第1の鍵を暗号化する暗号化ステップと、  
前記暗号化された情報、および前記暗号化ステップで暗号化された前記第1の鍵を前記記録媒体に記録する記録ステップとを含むことを特徴とする記録方法。

**【請求項 4】** 暗号化された情報、および前記情報を復号する第1の鍵を受信し、装着された記録媒体に前記情報を記録するとともに、第2の鍵を記憶する情報記憶媒体が装着される、記録装置に、  
前記情報記憶媒体と相互認証する相互認証ステップと、  
前記相互認証ステップでの前記相互認証に基づいて、前記情報記憶媒体から読み出された前記第2の鍵で、前記第1の鍵を暗号化する暗号化ステップと、  
前記暗号化された情報、および前記暗号化ステップで暗号化された前記第1の鍵を前記記録媒体に記録する記録ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

**【請求項 5】** 暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置において、  
前記記録媒体から読み出しされた前記鍵を復号する第1の復号手段と、  
前記第1の復号手段により復号された前記鍵で、前記暗号化された情報を復号する第2の復号手段とを備えることを特徴とする復号装置。

**【請求項 6】** 装着された、前記鍵を復号する第2の鍵が記憶されている情報記憶媒体と相互認証する相互認証手段をさらに備え、  
前記第1の復号手段は、前記相互認証手段が相互認証に基づいて得た前記第2の鍵で、前記暗号化された情報を復号する鍵を復号することを特徴とする請求項5に記載の復号装置。

**【請求項 7】** 暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置の復号方法において、

前記記録媒体から読み出しされた前記鍵を復号する第1の復号ステップと、  
前記第1の復号ステップで復号された前記鍵で、前記暗号化された情報を復号する第2の復号ステップとを含むことを特徴とする復号方法。

**【請求項 8】** 暗号化された情報、および前記情報を復号する暗号化された鍵が記録されている記録媒体が装着され、前記情報を復号する復号装置に、  
前記記録媒体から読み出しされた前記鍵を復号する第1の復号ステップと、  
前記第1の復号ステップで復号された前記鍵で、前記暗号化された情報を復号する第2の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

**【請求項 9】** 暗号化された情報を記録媒体に記録する記録装置、または暗号化されて前記記録媒体に記録された情報を復号する復号装置に装着される情報記憶媒体において、

前記記録装置または前記復号装置と相互認証する相互認証手段と、  
前記暗号化された情報を復号する第1の鍵を暗号化または復号する第2の鍵を記憶する記憶手段とを備えることを特徴とする情報記憶媒体。

**【請求項 10】** 前記記録媒体に記録された情報を復号する復号装置を特定するデータを記憶する第2の記憶手段をさらに備えることを特徴とする請求項9に記載の情報記憶媒体。

**【請求項 11】** 前記第2の鍵は、前記記録装置より供給されることを特徴とする請求項9に記載の情報記憶媒体。

**【請求項 12】** 前記第2の鍵は、前記復号装置より供給されることを特徴とする請求項9に記載の情報記憶媒体。

**【発明の詳細な説明】**

**【0001】**

**【発明の属する技術分野】** 本発明は、記録装置および方法、復号装置および方法、提供媒体、並びに情報記憶媒体に関し、特に、暗号化された情報を取り扱う記録装置および方法、復号装置および方法、提供媒体、並びに情

報記録媒体に関する。

【0002】

【従来の技術】不正な利用を防止するため音楽などの情報を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザは、その情報処理装置で情報を復号して、読み出しするシステムがある。一般に、契約にあたって、ユーザは、情報を利用する情報処理装置を特定するデータを、情報提供者に登録する。情報提供者は、その装置に限って、情報を利用できるように、情報を暗号化して提供する。

【0003】

【発明が解決しようとする課題】このようなシステムで供給された情報は、その情報が制限なく読み出しできる権利をユーザが取得したとしても、所定の契約を交わしたユーザが所有する他の読み出し装置では、利用できない。

【0004】本発明はこのような状況に鑑みてなされたものであり、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用できるようにすることを目的とする。

【0005】

【課題を解決するための手段】請求項1に記載の記録装置は、情報記憶媒体と相互認証する相互認証手段と、相互認証手段による相互認証に基づいて、情報記憶媒体から読み出された第2の鍵で、第1の鍵を暗号化する暗号化手段と、暗号化された情報、および暗号化手段により暗号化された第1の鍵を記録媒体に記録する記録手段とを備えることを特徴とする。

【0006】請求項3に記載の記録方法は、情報記憶媒体と相互認証する相互認証ステップと、相互認証ステップでの相互認証に基づいて、情報記憶媒体から読み出された第2の鍵で、第1の鍵を暗号化する暗号化ステップと、暗号化された情報、および暗号化ステップで暗号化された第1の鍵を記録媒体に記録する記録ステップとを含むことを特徴とする。

【0007】請求項4に記載の提供媒体は、記録装置に、情報記憶媒体と相互認証する相互認証ステップと、相互認証ステップでの相互認証に基づいて、情報記憶媒体から読み出された第2の鍵で、第1の鍵を暗号化する暗号化ステップと、暗号化された情報、および暗号化ステップで暗号化された第1の鍵を記録媒体に記録する記録ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0008】請求項5に記載の復号装置は、記録媒体から読み出された鍵を復号する第1の復号手段と、第1の復号手段により復号された鍵で、暗号化された情報を復号する第2の復号手段とを備えることを特徴とする。

【0009】請求項7に記載の復号方法は、記録媒体から読み出された鍵を復号する第1の復号ステップと、第1の復号ステップで復号された鍵で、暗号化された情

報を復号する第2の復号ステップとを含むことを特徴とする。

【0010】請求項8に記載の提供媒体は、復号装置に、記録媒体から読み出された鍵を復号する第1の復号ステップと、第1の復号ステップで復号された鍵で、暗号化された情報を復号する第2の復号ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0011】請求項9に記載の情報記憶媒体は、記録装置または復号装置と相互認証する相互認証手段と、暗号化された情報を復号する第1の鍵を暗号化または復号する第2の鍵を記憶する記憶手段とを備えることを特徴とする。

【0012】請求項1に記載の記録装置、請求項3に記載の記録方法、および請求項4に記載の提供媒体においては、情報記憶媒体と相互認証し、相互認証に基づいて、情報記憶媒体から読み出された第2の鍵で、第1の鍵を暗号化し、暗号化された情報、および暗号化された第1の鍵を記録媒体に記録する。

【0013】請求項5に記載の復号装置、請求項7に記載の復号方法、および請求項8に記載の提供媒体においては、記録媒体から読み出された鍵を復号し、復号された鍵で、暗号化された情報を復号する。

【0014】請求項9に記載の情報記憶媒体においては、相互認証手段が記録装置または復号装置と相互認証し、記憶手段が暗号化された情報を復号する第1の鍵を暗号化または復号する第2の鍵を記憶する。

【0015】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を附加して本発明の特徴を記述すると、次のようなになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0016】すなわち、請求項1に記載の記録装置は、情報記憶媒体と相互認証する相互認証手段（例えば、図1の相互認証部17）と、相互認証手段による相互認証に基づいて、情報記憶媒体から読み出された第2の鍵で、第1の鍵を暗号化する暗号化手段（例えば、図1の暗号化部15）と、暗号化された情報、および暗号化手段により暗号化された第1の鍵を記録媒体に記録する記録手段（例えば、図1の記録部12）とを備えることを特徴とする。

【0017】請求項5に記載の復号装置は、記録媒体から読み出された鍵を復号する第1の復号手段（例えば、図1の復号部32）と、第1の復号手段により復号された鍵で、暗号化された情報を復号する第2の復号手段（例えば、図1の復号部33）とを備えることを特徴とする。

【0018】請求項9に記載の情報記憶媒体は、記録装置または復号装置と相互認証する相互認証手段（例えば、図1の相互認証部22）と、暗号化された情報を復号する第1の鍵を暗号化または復号する第2の鍵を記憶する記憶手段（例えば、図1の記憶部21）とを備えることを特徴とする。

【0019】図1は、本発明の一実施の形態である記録読み出しシステムの構成を説明するブロック図である。受信記録装置1は、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化された音楽、映像、プログラム、文字等の情報（以下、コンテンツと称する）を提供するネットワークに接続されるとともに、コンテンツ鍵K<sub>con</sub>によりDESなどの共通鍵暗号方式で暗号化されているコンテンツ鍵K<sub>con</sub>が記録されているHDD2と、所定のバスを介して、情報を送受信する。受信記録装置1は、光ディスク5が装着され、装着された光ディスク5に暗号化されたコンテンツ等の所定のデータを記録させ、また、ICカード4が装着され、ICカード4が記憶する所定のデータを読み出す。

【0020】コンテンツを暗号化する共通鍵暗号方式であるDESは、56ビットの共通鍵を用い、平文の64ビットを1ブロックとして処理する暗号方式である。DESの処理は、平文を搅拌し、暗号文に変換する部分（データ搅拌部）と、データ搅拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DESのすべてのアルゴリズムは公開されているので、ここでは、データ搅拌部の基本的な処理を簡単に説明する。

【0021】まず、平文の64ビットは、上位32ビットのH<sub>0</sub>、および下位32ビットのL<sub>0</sub>に分割される。鍵処理部から供給された48ビットの拡大鍵K<sub>1</sub>、および下位32ビットのL<sub>0</sub>を入力とし、下位32ビットのL<sub>0</sub>をF関数で搅拌した出力が算出される。F関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の2種類の基本変換から構成されている。次に、上位32ビットのH<sub>0</sub>と、F関数の出力が排他的論理和され、その結果は下位32ビットL<sub>1</sub>とされる。下位32ビットL<sub>0</sub>は、上位32ビットH<sub>1</sub>とされる。

【0022】上位32ビットのH<sub>0</sub>および下位32ビットのL<sub>0</sub>を基に、以上の処理を16回繰り返し、得られた上位32ビットのH<sub>16</sub>および下位32ビットのL<sub>16</sub>が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0023】通信部11は、ネットワークに情報を送信し、ネットワークから情報を受信する。記憶部12は、光ディスク5が装着されたとき、装着された光ディスク12に暗号化部15またはHDD2から供給された情報を記録させる。記憶部13は、コンテンツ鍵K<sub>con</sub>を復

号する保存用鍵K<sub>s</sub>を記憶する。復号部14は、HDD2に記録されているコンテンツ鍵K<sub>con</sub>を、記憶部13が記憶する保存用鍵K<sub>s</sub>で復号する。暗号化部15は、復号部14で復号されたコンテンツ鍵K<sub>con</sub>を、ICカードインターフェース16を介して、ICカード4から供給された移動用鍵K<sub>t</sub>で暗号化する。

【0024】ICカードインターフェース16は、受信記録装置1に装着されたICカード4から供給された所定のデータを、所定の形式に変更し、暗号化部15、ID識別部18、または相互認証部17に出力し、また、暗号化部15、ID識別部18、または相互認証部17から供給された所定のデータを、所定の形式に変更し、装着されたICカード4に出力する。相互認証部17は、ICカードインターフェース16を介して、DESなどの共通鍵暗号を使用して後述する手続により、ICカード4と相互認証する。ID(Identification Data)識別部18は、ICカードインターフェース16を介して、ICカード4から供給された、そのICカード4に固有のIDを基に、ICカード4を識別する。

【0025】ICカード4は、読み出し装置3と1対1の組み合わせで、共に販売され、受信記録装置1に着脱自在な構造を有し、受信記録装置1に装着したとき、対応する読み出し装置3固有のIDを供給し、ICカード4を識別させ、相互認証し、移動用鍵K<sub>t</sub>を供給する。ICカード4は、記憶部21、相互認証部22、およびID記憶部23を備える。記憶部21は、ROM(Read Only Memory)、不揮発性メモリ(EEPROM(Electric Erasable Program ROM)、フラッシュメモリ、FRAM(商標)(Ferroelectric Random Access Memory)等)で構成され、移動用鍵K<sub>t</sub>が記憶されている。相互認証部22は、ICカードインターフェース16を介して、DESなどの共通鍵暗号を使用して後述する手続により、受信記録装置1と相互認証する。ID記憶部23は、ROMで構成され、そのICカード4に対応する、読み出し装置3に固有のIDを記憶する。

【0026】受信記録装置1とバスおよびネットワークで接続されていない、例えば、自動車に取り付けられ、またはユーザが携帯して使用する読み出し装置3は、読み出し部31、復号部32、復号部33、および記憶部34を備える。読み出し部31は、受信記録装置1により、暗号化されたコンテンツおよびコンテンツ鍵K<sub>con</sub>が記録された光ディスク5が装着されたとき、光ディスク5に記録されたコンテンツおよびコンテンツ鍵K<sub>con</sub>を読み出します。復号部32は、読み出し部31が光ディスク5から読み出したコンテンツ鍵K<sub>con</sub>を、記憶部34が記憶する移動用鍵K<sub>t</sub>で復号し、復号したコンテンツ鍵K<sub>con</sub>を復号部33に供給する。復号部33は、読み出し部31が光ディスク5から読み出したコンテンツを、復号部32から供給されたコンテンツ鍵K<sub>con</sub>で復号する。記憶部34は、ICカード4の記憶

部21に記憶された移動用鍵K<sub>t</sub>と同一の移動用鍵K<sub>t</sub>を記憶する。

【0027】HDD2は、バスにより受信記録装置1と接続され、コンテンツ鍵K<sub>c o n</sub>によりDESなどの共通鍵暗号方式で暗号化されているコンテンツ、および保存用鍵K<sub>s</sub>で暗号化されているコンテンツ鍵K<sub>c o n</sub>を記録している。

【0028】次に図2のフローチャートを参照して、受信記録装置1が、HDD2が記録しているコンテンツ等を光ディスク5に記録する処理を説明する。ステップS11において、受信記録装置1のICカードインターフェース16には、ICカード4が装着される。ステップS12において、受信記録装置1の記録部12には、光ディスク5が装着される。ステップS13において、受信記録装置1のID識別部18は、ICカードインターフェース16を介して、ICカード4のID記憶部23に記憶された読み出し装置3のIDを読み出す。ステップS14において、受信記録装置1のID識別部18は、ICカード4のID記憶部23から読み出されたIDが、ID識別部18に登録されているか否かを判定し、IDがID識別部18に登録されていると判定された場合、ステップS15に進み、相互認証部17は、ICカード4の相互認証部22と相互認証する。相互認証の処理の詳細は、図3のフローチャートを用いて後述する。

【0029】ステップS16において、相互認証部17は、ステップS15においてICカード4と相互認証できたか否かを判定し、ICカード4と相互認証できたと判定された場合、ステップS17に進み、復号部14は、HDD2から、保存用鍵K<sub>s</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を読み出す。ステップS18において、復号部14は、読み出した、暗号化されているコンテンツ鍵K<sub>c o n</sub>を、記憶部13に記憶されている保存用鍵K<sub>s</sub>で復号し、復号したコンテンツ鍵K<sub>c o n</sub>を暗号化部15に供給する。

【0030】ステップS19において、暗号化部15は、ICカードインターフェース16を介して、ICカード4の記憶部21が記憶する移動用鍵K<sub>t</sub>を読み出す。ステップS20において、暗号化部15は、復号されたコンテンツ鍵K<sub>c o n</sub>を、移動用鍵K<sub>t</sub>で、再度、暗号化し、暗号化されたコンテンツ鍵K<sub>c o n</sub>を記録部12に供給する。ステップS21において、記録部12は、移動用鍵K<sub>t</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を光ディスク5に記録する。ステップS22において、記録部12は、HDD2から、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツを読み出す。ステップS23において、記録部12は、ステップS22で読み出されたコンテンツを光ディスク5に記録し、処理を終了する。

【0031】ステップS14において、ICカード4のID記憶部23から読み出されたIDが、ID識別部18に登録されていないと判定された場合、およびステップS16

において、ICカード4と相互認証されなかったと判定された場合、ステップS24に進み、ID識別部18または相互認証部17は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【0032】以上のように、受信記録装置1は、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツ、および移動用鍵K<sub>t</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を光ディスク5に記録する。

【0033】次に図3のフローチャートを参照して、図2のステップS15に対応して、2つの共通鍵K<sub>c 1</sub>、K<sub>c 2</sub>で、共通鍵暗号であるDESを用いて行われる、受信記録装置1とICカード4の相互認証の処理の詳細を説明する。ステップS31において、受信記録装置1の相互認証部17は、64ビットの乱数R1を生成する。ステップS32において、受信記録装置1の相互認証部17は、乱数R1を予め記憶している共通鍵K<sub>c 1</sub>で暗号化する。ステップS33において、受信記録装置1の相互認証部17は、暗号化された乱数R1をICカード4の相互認証部22に送信する。

【0034】ステップS34において、ICカード4の相互認証部22は、受信した乱数R1を予め記憶している共通鍵K<sub>c 1</sub>で復号する。ステップS35において、ICカード4の相互認証部22は、乱数R1を予め記憶している共通鍵K<sub>c 2</sub>で暗号化する。ステップS36において、ICカード4の相互認証部22は、64ビットの乱数R2を生成する。ステップS37において、ICカード4の相互認証部22は、乱数R2を共通鍵K<sub>c 2</sub>で暗号化する。ステップS38において、ICカード4の相互認証部22は、暗号化された乱数R1および乱数R2を受信記録装置1の相互認証部17に送信する。

【0035】ステップS39において、受信記録装置1の相互認証部17は、受信した乱数R1および乱数R2を予め記憶している共通鍵K<sub>c 2</sub>で復号する。ステップS40において、受信記録装置1の相互認証部17は、復号した乱数R1を調べ、ステップS31で生成した乱数R1（暗号化する前の乱数R1）と一致すれば、ICカード4を適正なICカードとして認証し、一致しなければ、不正なICカードであるとして、処理を終了する。ステップS41において、受信記録装置1の相互認証部17は、復号して得た乱数R2を共通鍵K<sub>c 1</sub>で暗号化する。ステップS42において、受信記録装置1の相互認証部17は、暗号化された乱数R2をICカード4の相互認証部22に送信する。

【0036】ステップS43において、ICカード4の相互認証部22は、受信した乱数R2を共通鍵K<sub>c 1</sub>で復号する。ステップS44において、ICカード4の相互認証部22は、復号した乱数R2が、ステップS36で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、受信記録装置1を適正な受信記録装置として認証

し、一致しなければ、不正な受信記録装置であるとして処理を終了する。

【0037】図4は、読み出し装置3がコンテンツを復号する処理を説明するフローチャートである。ステップS51において、読み出し装置3の読み出し部31は、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツ、および移動用鍵K<sub>t</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>が記録された光ディスク5が装着される。ステップS52において、読み出し部31は、装着された光ディスク5から、移動用鍵K<sub>t</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を読み出し、復号部32に供給する。ステップS53において、復号部32は、記憶部34に記憶された移動用鍵K<sub>t</sub>を読み出す。ステップS54において、復号部32は、移動用鍵K<sub>t</sub>でコンテンツ鍵K<sub>c o n</sub>を復号し、復号部33に供給する。ステップS55において、読み出し部31は、装着された光ディスク5から、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツを読み出し、復号部33に供給する。ステップS56において、復号部33は、コンテンツ鍵K<sub>c o n</sub>でコンテンツを復号し、処理は終了する。

【0038】このように、読み出し装置3は、光ディスク5に記録されたコンテンツを復号する。

【0039】図5は、本発明の他の実施の形態である記録読み出しシステムの構成を説明するブロック図である。図5に示す受信記録装置1は、図1に示す受信記録装置1に対して、記憶部13、復号部14、暗号化部15、ICカードインターフェース16、相互認証部17、およびID識別部18が省略された構成を有する。

【0040】図5に示すICカード4は、図1に示したICカード4と同様の構成を有するが、記憶部21は、コンテンツ鍵K<sub>c o n</sub>を暗号化した（復号できる）保存用鍵K<sub>s</sub>を記憶する。

【0041】図5に示す読み出し装置3は、図1に示された読み出し装置3に対して、記憶部34が省略され、ICカードインターフェース41、相互認証部42、およびID識別部43が加えられた構成を有する。ICカードインターフェース41、相互認証部42、およびID識別部43の機能は、図1に示された受信記録装置1のICカードインターフェース16、相互認証部17、およびID識別部18と、それぞれ同様であるので、その説明は省略する。

【0042】次に図6のフローチャートを参照して、図5に示す受信記録装置1が、HDD2が記録しているコンテンツ等を光ディスク5に記録する処理を説明する。ステップS61において、受信記録装置1の記録部12は、光ディスク5が装着される。ステップS62において、記録部12は、HDD2から、保存用鍵K<sub>s</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を読み出す。ステップS63において、記録部12は、暗号化されたコンテンツ鍵K<sub>c o n</sub>を光ディスク5に記録する。ステップS64に

おいて、記録部12は、HDD2から、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツを読み出す。ステップS65において、記録部12は、光ディスク5に暗号化されたコンテンツを記録する。

【0043】このように、図5に示した受信記録装置1は、光ディスク5に暗号化されたコンテンツおよび保存用鍵K<sub>s</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を記録する。

【0044】さらに図7のフローチャートを参照して、図5に示す読み出し装置3が、コンテンツを復号する処理を説明する。ステップS71において、読み出し装置3のICカードインターフェース41には、ICカード4が装着される。ステップS72において、読み出し装置3の読み出し部31には、光ディスク5が装着される。ステップS73において、読み出し装置3のID識別部43は、ICカードインターフェース41を介して、ICカード4のID記憶部23に記憶された読み出し装置3のIDを読み出す。ステップS74において、読み出し装置3のID識別部43は、ICカード4のID記憶部23から読み出されたIDが、ID識別部43に登録されているか否かを判定し、IDがID識別部43に登録されていると判定された場合、ステップS75に進み、相互認証部42は、ICカード4の相互認証部22と相互認証する。相互認証の処理の詳細は、図3のフローチャートを用いて説明したものと同様であるので、その説明は省略する。

【0045】ステップS76において、相互認証部42は、ステップS75においてICカード4と相互認証できたか否かを判定し、ICカード4と相互認証できたと判定された場合、ステップS77に進み、読み出し部31は、装着された光ディスク5から、保存用鍵K<sub>s</sub>で暗号化されたコンテンツ鍵K<sub>c o n</sub>を読み出し、復号部32に供給する。ステップS78において、復号部32は、ICカードインターフェース41を介して、ICカード2の記憶部21から、保存用鍵K<sub>s</sub>を読み出す。ステップS79において、復号部32は、コンテンツ鍵K<sub>c o n</sub>を保存用鍵K<sub>s</sub>で復号する。ステップS80において、読み出し部31は、装着された光ディスク5から、コンテンツ鍵K<sub>c o n</sub>で暗号化されたコンテンツを読み出し、復号部33に供給する。ステップS81において、復号部33は、コンテンツ鍵K<sub>c o n</sub>でコンテンツを復号し、処理は終了する。

【0046】ステップS74において、読み出されたIDがID識別部43に登録されていないと判定された場合、およびステップS76において、ICカード4と相互認証できなかったと判定された場合、ステップS82に進み、ID識別部43または相互認証部42は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【0047】以上のように、図5に示した読み出し装置3は、光ディスク5に記録されたコンテンツを復号す

る。

【0048】図8は、移動用鍵K<sub>t</sub>を読み出し装置3のみが有する場合の、記録読み出しシステムの構成を説明するブロック図である。図8に示す受信記録装置1は、図1に示す場合と同様であるので、その説明は省略する。ICカード4の記憶部21は、EEPROM(Electrically Erasable Programmable Read Only Memory)、フラッシュメモリ、強誘電体メモリなどの電気的に記憶内容を書き換えできる、汎用の不揮発性メモリで構成され、ICカード4が読み出し装置3に装着されたとき、コンテンツ鍵K<sub>con</sub>を暗号化する移動用鍵K<sub>t</sub>を記憶するようになされている。図8に示す読み出し装置3は、図5に示す場合と、ほぼ同様あり、その説明は適宜省略する。図8のICカードインターフェース41は、相互認証部42、およびID識別部43に対する動作は、図5に示す場合と同様であるが、記憶部34に対しては、記憶部34に記憶された移動用鍵K<sub>t</sub>をICカード4の記憶部21に記憶させる動作をすることが、図5に示す場合と異なる。

【0049】図9のフローチャートを参照して、図8に示す読み出し装置3が、ICカード4に移動用鍵K<sub>t</sub>を記憶させる処理を説明する。ステップS91において、読み出し装置3のICカードインターフェース41には、ICカード4が装着される。ステップS92において、読み出し装置3のID識別部43は、ICカードインターフェース41を介して、ICカード4のID記憶部23に記憶された読み出し装置3のIDを読み出す。ステップS93において、読み出し装置3のID識別部43は、ICカード4のID記憶部23から読み出された読み出し装置3のIDが、ID識別部43に登録されているか否かを判定し、読み出し装置3のIDがID識別部43に登録されていると判定された場合、ステップS94に進み、相互認証部42は、ICカード4の相互認証部22と相互認証する。相互認証の処理の詳細は、図3のフローチャートを用いて説明したものと同様であるので、その説明は省略する。

【0050】ステップS95において、相互認証部42は、ステップS94においてICカード4と相互認証できなかったか否かを判定し、ICカード4と相互認証できたと判定された場合、ステップS96に進み、記憶部34は、移動用鍵K<sub>t</sub>をICカード4の記憶部21に記憶させ、処理は終了する。

【0051】ステップS93において、読み出されたIDがID識別部43に登録されていないと判定された場合、およびステップS95において、ICカード4と相互認証できなかつたと判定された場合、ステップS97に進み、ID識別部43または相互認証部42は、所定のエラーメッセージを図示せぬディスプレイに表示するなどの所定のエラー処理を実行し、処理は終了する。

【0052】以上の処理により、移動用鍵K<sub>t</sub>は、ICカード4の記憶部21に記憶される。図8に示す受信記録

装置1が、光ディスク5に暗号化されたコンテンツを記録する処理は、図2のフローチャートで説明した処理と同様である。図8に示す読み出し装置が、光ディスク5に記録されたコンテンツを復号する処理は、図4のフローチャートで説明した処理と同様である。

【0053】図10は、保存用鍵K<sub>s</sub>を受信記録装置1のみが有する場合の、記録読み出しシステムの構成を説明するブロック図である。図10に示す読み出し装置3は、図5に示す場合と同様であるので、その説明は省略する。図10に示すICカード4は、図8に示す場合と、同様であるので、その説明は省略する。図10に示す受信記録装置1は、図1に示す受信記録装置1に対して、復号部14、および暗号化部15が省略された構成を有する。図10に示す受信記録装置1の記憶部51は、コンテンツ鍵K<sub>con</sub>を暗号化した（コンテンツ鍵K<sub>con</sub>を復号できる）保存用鍵K<sub>s</sub>を記憶し、保存用鍵K<sub>s</sub>をICカードインターフェース16に供給するようになされている。

【0054】図10の記録読み出しシステムにおいては、受信記録装置1に、ICカード4が装着されたとき、図9のフローチャートと同様の処理で、受信記録装置1の記憶部51が記憶する保存用鍵K<sub>s</sub>が、ICカード4に記憶される。図10に示す受信記録装置1が、光ディスク5に暗号化されたコンテンツを記録する処理は、図6のフローチャートで説明した処理と同様である。図10に示す読み出し装置3が、光ディスク5に記録されたコンテンツを復号する処理は、図7のフローチャートで説明した処理と同様である。

【0055】以上のように、コンテンツの不正な使用を防止しつつ、所定の読み出し装置で、コンテンツを利用できる。

【0056】なお、相互認証の処理として、共通鍵暗号方式であるDESで、2つの鍵を使用する処理を説明したが、DESで、1つの鍵を使用する処理、NTT(商標)が提案するFEAL、IDEA(International Data Encryption Algorithm)を使用する処理、またはRAS(Rivest-Shamir-Adleman)暗号などの公開鍵暗号を使用する処理でもよい。

【0057】また、コンテンツはDESで暗号化されるとして説明したが、FEAL、またはIDEAなどの他の共通鍵暗号方式、並びにRASなど公開鍵暗号方式で暗号化してもよい。

【0058】暗号化されたコンテンツおよび暗号化されたコンテンツ鍵K<sub>con</sub>は、光ディスク5に記録するとして説明したが、フロッピディスク、MD(Mini Disk:商標)、磁気テープなどの記録媒体でもよい。

【0059】また、ICカード4のID記憶部23から読み出されたIDが、ID識別部18またはID識別部43に登録されていないとき、エラー処理をして終了すると説明したが、ID識別部18またはID識別部43に不正なIDを記

憶しておき、それと同一のIDがICカード4のID記憶部23から読み出されたときも、エラー処理をして終了するようにしてよい。

【0060】なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0061】また、上記したような処理を行うコンピュータプログラムをユーザーに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができます。

#### 【0062】

【発明の効果】請求項1に記載の記録装置、請求項3に記載の記録方法、および請求項4に記載の提供媒体によれば、情報記憶媒体と相互認証し、第2の鍵で、第1の鍵を暗号化し、暗号化された情報、および暗号化された第1の鍵を記録媒体に記録するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用することが可能になる。

【0063】請求項5に記載の復号装置、請求項7に記載の復号方法、および請求項8に記載の提供媒体によれば、記録媒体から読み出しされた鍵を復号し、復号された鍵で、暗号化された情報を復号するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置以外で利用することが可能になる。

【0064】請求項9に記載の情報記憶媒体によれば、記録装置または復号装置と相互認証するとともに、暗号化された情報を復号する第1の鍵を暗号化または復号する第2の鍵を記憶するようにしたので、不正な利用を防止しつつ、暗号化された情報を、情報が供給された装置

以外で利用することが可能になる。

#### 【図面の簡単な説明】

【図1】記録読み出しシステムの構成を説明するブロック図である。

【図2】受信記録装置1が、HDD2が記録しているコンテンツ等を光ディスク5に記録する処理を説明するフローチャートである。

【図3】受信記録装置1とICカード4の相互認証の処理の詳細を説明するフローチャートである。

【図4】読み出し装置3がコンテンツを復号する処理を説明するフローチャートである。

【図5】記録読み出しシステムの構成を説明するブロック図である。

【図6】図5に示す受信記録装置1が、HDD2が記録しているコンテンツ等を光ディスク5に記録する処理を説明するフローチャートである。

【図7】図5に示す読み出し装置3が、コンテンツを復号する処理を説明するフローチャートである。

【図8】記録読み出しシステムの構成を説明するブロック図である。

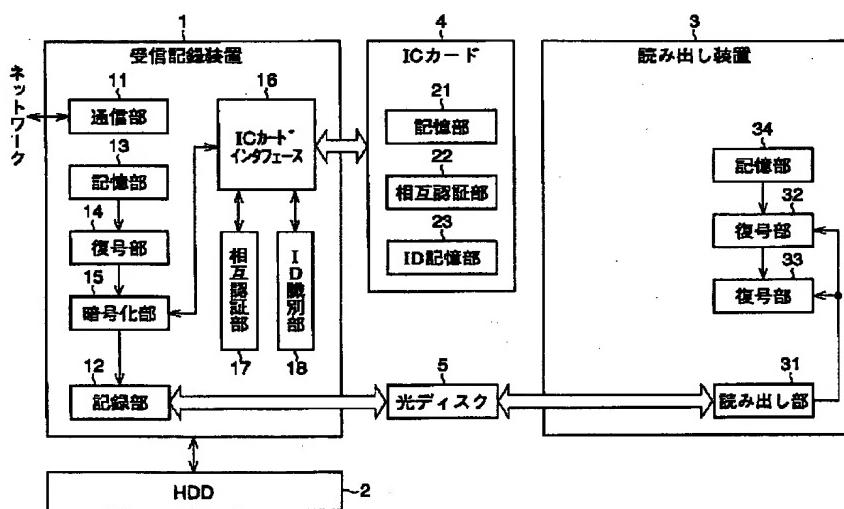
【図9】ICカード4に移動用鍵Ktを記憶させる処理を説明するフローチャートである。

【図10】記録読み出しシステムの構成を説明するブロック図である。

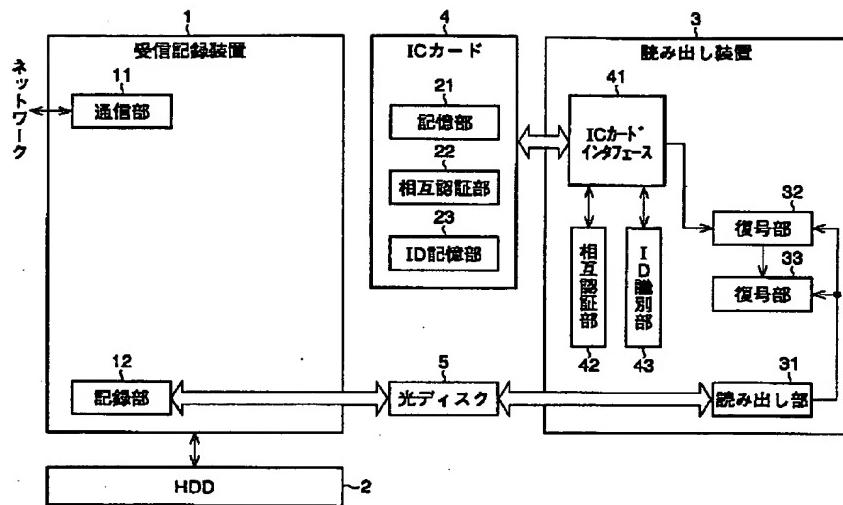
#### 【符号の説明】

- 1 受信記録装置, 2 HDD, 3 読み出し装置,
- 4 ICカード, 5 光ディスク, 12 記憶部,
- 15 暗号化部, 17 相互認証部, 21 記憶部,
- 22 相互認証部, 23 ID記憶部, 24 記憶部,
- 32 復号部, 33 復号部, 34 復号部

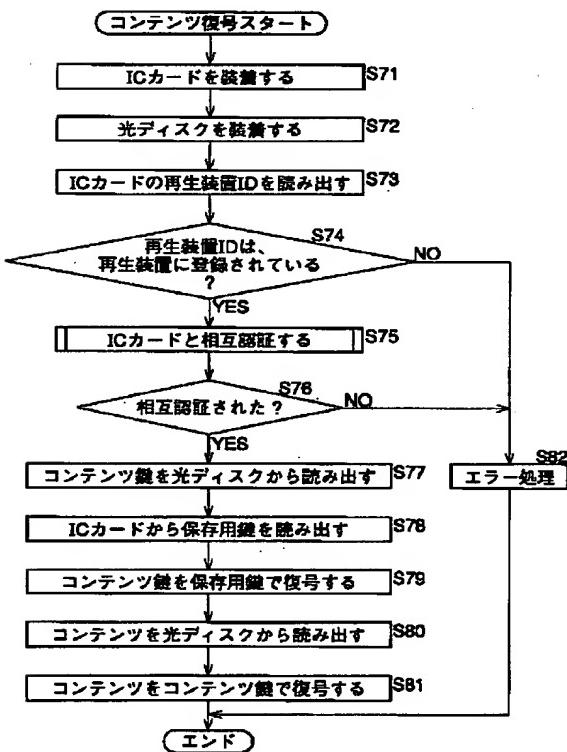
【図1】



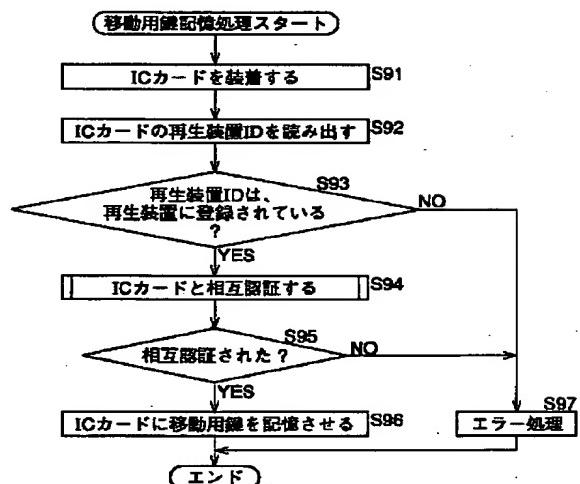
【図 5】



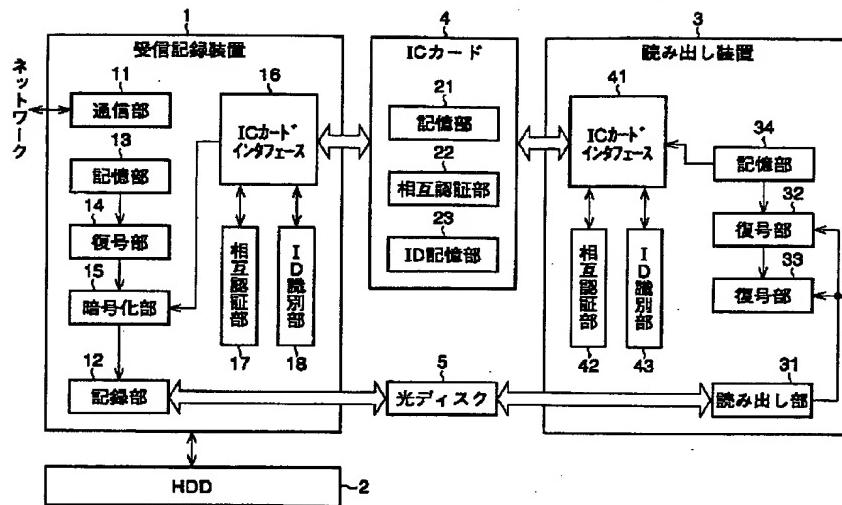
【図 7】



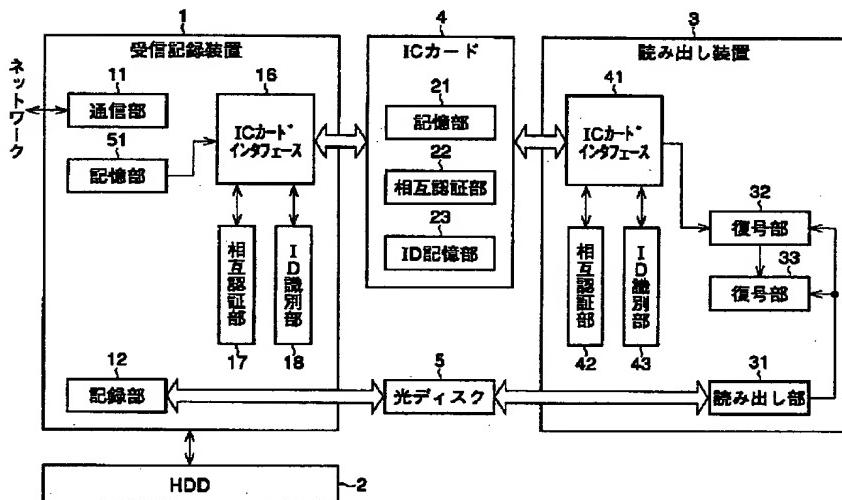
【図 9】



【図 8】



【図 10】



フロントページの続き

(72) 発明者 北村 出  
東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

(72) 発明者 北原 淳  
東京都品川区北品川6丁目7番35号 ソニ  
一株式会社内

Fターム(参考) 5D044 BC06 CC04 CC08 DE49 GK17  
HH02 HL11  
5K013 BA03 FA06 GA02 GA05